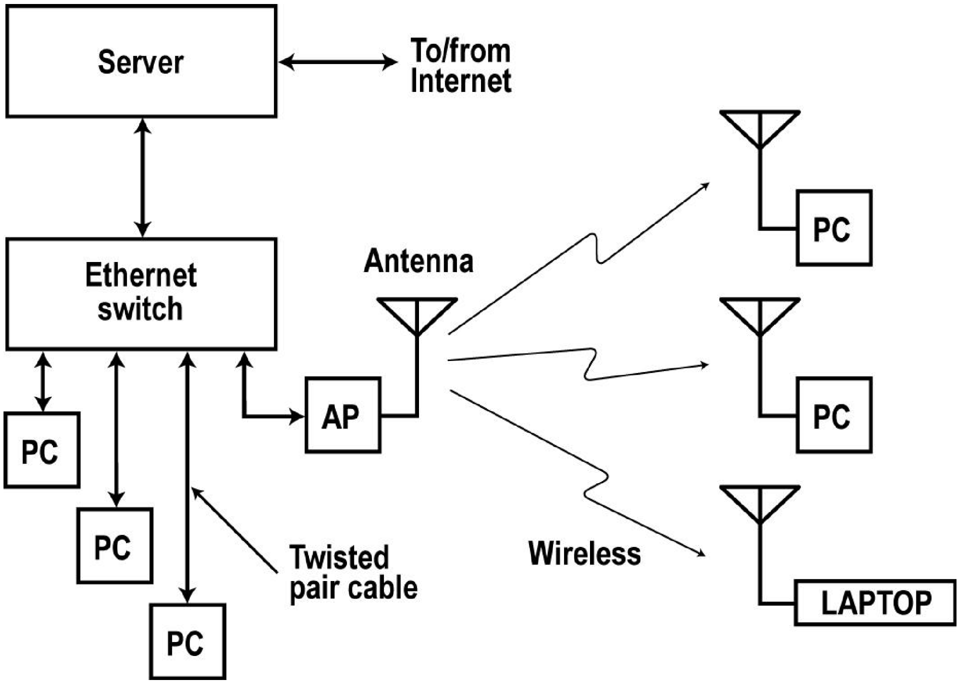
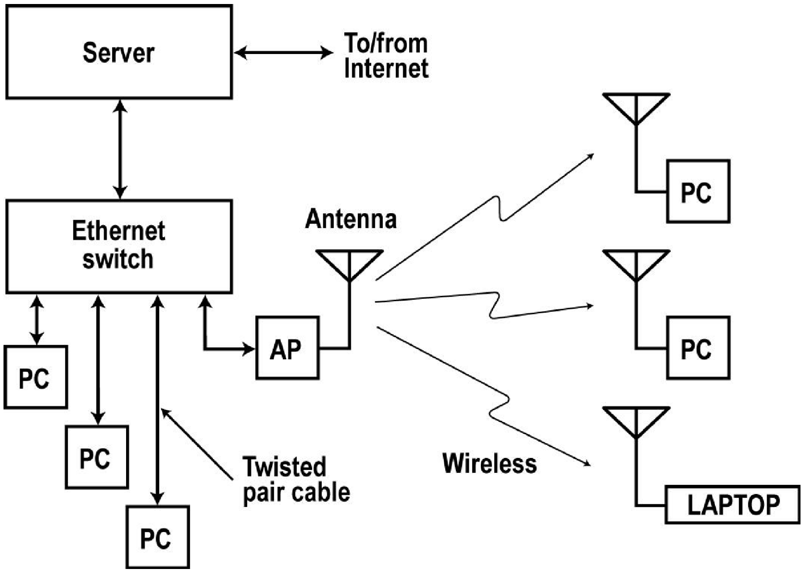
Wireless Local Area Networks

Wireless Local Area Networks



Wireless local area networks (WLANs) are interconnections of personal computers (PCs), laptops, personal digital assistants (PDAs), and other devices by radio.

WLAN

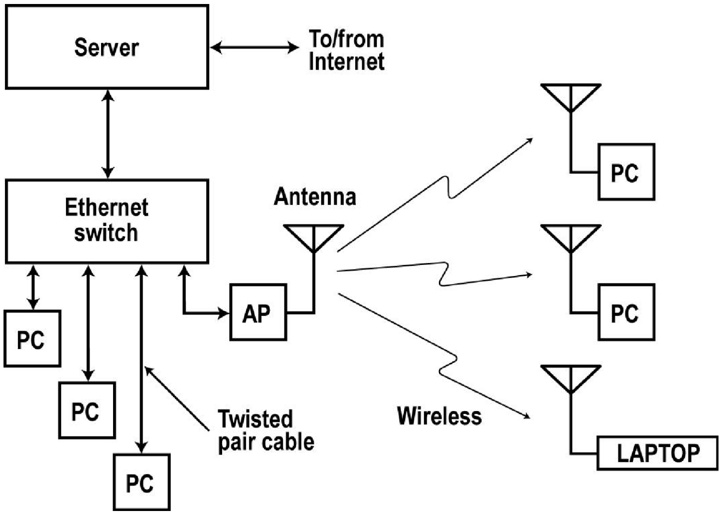


A wired local area network (LAN) is a collection of PCs connected together usually by twisted pair cable using the Ethernet standard. The PCs connect to an Ethernet switch that in turn communicates with the server, a computer than manages the network. The LAN allows individual users to access the Internet, perform email, and share company resources like data bases and printers.

Wireless Access Points

Wired LANs can be extended by adding one or more wireless access points (APs) through a two-way radio transceiver. Extra computers can be added to the system by allowing them access by radio.

The computers contain a wireless adapter or wireless network interface card (NIC) that are two-way data radios or transceivers that communicate with the access point.



Hot Spots

Another popular variation of a WLAN is the so called “hot spot”.

A hot spot is an access point installed in some public location such as an airport, hotel, coffee shop, restaurant, park, or other location. Users with a laptop computer with a wireless adapter card can link up with the hot spot to have access to the Internet, email, or other services.

The hot spot communicates back to an Internet service provider (ISP) by way of a high speed telephone line called a T1 line or by some other wireless connection.

There are over 20,000 hot spots in the US and the number is growing.

Home Networking

Many homes today have two or more PCs. Home networks are used so that the PCs may share a common high speed Internet service, a printer, or other resources.

Conventional wired Ethernet LANs may be installed but since most homes do not have the required twisted pair wiring, a wireless network makes more sense.

A typical home network consists of a wireless gateway or router that connects to the high speed Internet line. The cable TV or DSL modem plugs into the router or gateway. The router communicates wirelessly with each PC or laptop that contains a wireless adapter or NIC.

WLAN Standards

The WLAN standards are set and maintained by the Institute of Electrical and Electronic Engineers (IEEE).

The primary standard is called 802.11. Several different versions are available.

The 802.11b standard defines a WLAN that operates in the 2.4 to 2.483 GHz band. The band is divided up into eleven 20 MHz wide overlapping channels.

WLAN Standards: Transmission

This standard uses direct sequence spread spectrum (DSSS) with different forms of modulation depending upon the data rate.

The maximum data rate is 11 Mbps but this decreases to 5.5, 2, or 1 Mbps as the range is increased or as noise and interference is encountered.

The maximum transmission range is about 300 feet outdoors but this varies with the environment and greatly decreases indoors as the radio signal is absorbed as it passes through walls, etc.

This was the original WLAN standard and is still widely used but has been mostly replaced by the newer 802.11g standard.

802.11g

A newer version of the WLAN standard is called 802.11g.

It uses the same 2.4 GHz frequency band.

This standard defines the use of orthogonal frequency division multiplexing (OFDM) a special broad modulation scheme that inherently includes multiplexing.

The maximum data rate is 54 Mbps but it drops off to 48, 24, 12, 6 Mbps or less depending upon range, noise level, and interference.

The maximum range is 300 feet outdoors and less indoors.

Most new WLANs use this standard. A Linksys 802.11g router is shown here.

Photo coutesy of Linksys, a division of Cisco systems

802.11a

The 802.11a standard operates in the 5.8 GHz band. There is less interference from other WLANs or other radio services.

This standard defines OFDM and a maximum data rate of 54 Mbps.

The maximum range is about 100 feet.

Some access points and wireless adapter cards include transceivers for both standards.

Additional Standards

A newer WLAN standard (802.11n) is being developed. It defines an even faster data from 100 Mbps to 250 Mbps depending upon the range, noise, and interference. It uses multiple radios with multiple antennas operating at the same time.

The 802.11i standard defines high level encryption scheme to provide security to wireless transmissions.

Many other versions are defined. For more information on the standards and status of new version, go to the Institute of Electrical and Electronic Engineers (IEEE) website and look under Standards then 802.

Wi-Fi

Wi-Fi means wireless fidelity and is the trademark of the Wi-Fi Alliance. This is an organization of semiconductor chip companies, WLAN equipment manufacturers, and software vendors that develop and sell 802.11 products.

The Wi-Fi Alliance sponsors a certification and testing program for WLAN equipment to ensure that all the equipment of one vendor will work with all other vendor’s equipment.

While the standards generally ensure interoperability between different equipment, there are enough variations in actual hardware and software implementation to prevent full compatibility. The Wi-Fi certification ensures full compliance and interoperability.

Other WLAN Applications

Most 802.11 equipment is used in a LAN or WLAN, a hot spot, or a home network. However, there are other applications.

WLAN equipment can also be used in telemetry applications. Telemetry means measurement at a distance. By using sensors to measure temperature, pressure, light level, or other physical characteristics and converting this measurement to digital, it can be transmitted by a Wi-Fi transceiver to a central collection point where the data can be stored, analyzed, or even used in control operations.

WLAN hardware can also be used in surveillance where voice or video from microphones and cameras can be digitized and transmitted as data by Wi-Fi to a remote monitoring point.

Wi-Fi has also been used as a broadband access system where high speed Internet connections can be provided to homes where no cable TV or DSL service is available.

The Security Issue

It is possible to monitor and intercept wireless data with a nearby receiver or wireless adapter on a laptop. Hackers have been known to steal data or have unauthorized access to credit card numbers or other sensitive information.

The 802.11 standard has a built in encryption method called Wired Equivalent Protection (WEP). If WEP is enabled, some protection is provided. However, WEP encryption can be broken.

The Wi-Fi Alliance has better encryption methods called Wireless Protected Access (WPA) or a newer better version called WPA2. Some vendors also have their own proprietary encryption methods.

The IEEE 802.11i standard defines even stronger protection methods thereby reducing the risk of unauthorized monitoring.

With encryption, security is no longer an issue preventing the use of WLANs.

Test your knowledge

Contemporary Wireless Technology

Knowledge Probe 4

Wireless Local Area Networks

Click on Course Materials at the top of the page.

Then choose **Knowledge Probe 4**.